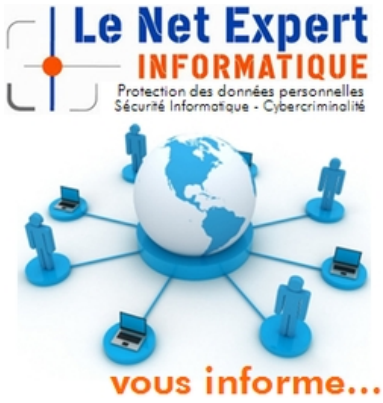
Les objets connectés deviendraient des témoins ? | Le Net Expert Informatique



Les objets connectés deviendraient des témoins ?

Aux Etats-Unis, on commence à produire les données de bracelets connectés pour démentir ou renforcer un témoignage. Ces données pourraient aussi entrer dans nos tribunaux, ce qui n'est pas sans poser question.

A quoi servent les objets connectés « portables », ces bracelets ou ces montres qui permettent de mesurer votre activité physique, vos dépenses en calories et même parfois votre humeur ?
A mieux se connaître, répondent les amateurs. A mener une vie plus saine. Mais une histoire récente, aux Etats-Unis, montre que ces objets peuvent aussi servir lors de votre procès.

Et là, son FitBit a lâché le morceau
Une femme de 43 ans qui avait porté plainte pour viol a été démentie par les données de son FitBit (bracelet connecté mesurant l'activité et le sommeil). L'histoire a été rapportée la semaine dernière par la chaîne d'information locale ABC 27 News.
La femme avait affirmé aux enquêteurs qu'un homme s'était introduit au milieu de la nuit dans sa chambre et l'avait menacée avec un couteau avant de la violer. Mais son gadget a contesté ses dires :
« Elle avait affirmé qu'elle avait perdu sa montre de fitness en résistant à son agresseur, mais l'objet a été retrouvé intact dans le couloir, près de la salle de bains [où elle avait dit que s'était déroulé le viol, ndlr].
Selon le chef d'inculpation, quand les enquêteurs ont téléchargé son activité de fitness, ils se sont aperçus que la femme n'avait pas dormi cette nuit-là et qu'elle avait marché tout le temps, au lieu de dormir comme elle l'avait affirmé. »
En plus de ces données, les enquêteurs n'ont trouvé aucune trace de pas dans la neige autour de la maison (les faits se sont déroulés en mars) ni aucune trace d'intrusion. En conséquence, la femme a été inculpée pour fausse déclaration et altération de preuves.

Des grosses balances, ces Google Glass
Déjà, en novembre 2014, à Calgary (Canada), une femme, qui demandait à être indemnisée pour préjudice corporel après un accident, a utilisé les données de son bracelet connecté pour prouver que son activité physique était réduite depuis son accident. (Une histoire alors analysée par Olivier Ertzscheid.)

Les objets connectés arrivent donc dans les tribunaux. Et selon les avocats cités dans la presse américaine (ici ou ici, par exemple), cette tendance est appelée à grandir. Dans Wired, un avocat américain se demandait ainsi :
« [Les données des objets connectés] pourraient-elles être utilisées comme alibi ? »
Ou encore :
« Est-ce qu'on pourrait utiliser les données d'un FitBit pour prouver qu'un cardiologue avait fait preuve de négligence, en ne restreignant pas l'exercice d'un patient ? »
Ces objets peuvent donner des indications sur les activités de celui ou celle qui le porte, mais aussi sur le lieu où il ou elle se trouve, grâce à des fonctions de géolocalisation. Les plus sophistiqués, comme les Google Glass, font aussi des photos ou des vidéos, ainsi que des recherches sur le Web.
On voit bien l'usage que policiers, assureurs ou autres pourraient faire de ces données, en les retournant contre son propriétaire.

Bientôt dans nos prétoires
En France, le cas ne s'est encore jamais présenté, mais, explique Me Clarisse Le Corre, avocate au cabinet Vigo, il est tout à fait envisageable :
« Selon la loi, les infractions peuvent être établies par tous modes de preuve et c'est le juge qui décide ensuite selon son intime conviction. »
A cheval entre données personnelles et données médicales, ces informations sont souvent appelées « données de bien-être ». Elles sont protégées par la loi « Informatique et libertés », mais dans le cas d'un procès, cette protection peut être levée par l'instruction.
Pourvu qu'elles soient légalement recevables et qu'elles soient ensuite soumises au contradictoire, c'est-à-dire être débattues par les deux parties, les données des objets connectés peuvent tout à fait être présentées devant un tribunal.

Leurs données sont-elles fiables ?
Pourtant, ces données sont loin d'être totalement fiables.
Les objets connectés buguent.
Comme l'a récemment montré notre collègue Thibaut Schepman, les appareils connectés peuvent bugger et les données récoltées ne reflètent pas forcément vos activités.

Ils sont faciles à duper.
Pas besoin de réfléchir longtemps pour voir comment on pourrait duper le bracelet connecté : il suffit de le faire porter par un complice ou de l'apposer à un animal domestique au comportement pas trop erratique. Ou encore de rester assis à son bureau en bougeant les pieds très vite pour faire croire qu'on fait un jogging.

Ils « mesurent » selon des critères qui changent de machine en machine et sont déterminés par des algorithmes inaccessibles.
Comme le rappelle la chercheuse américaine Kate Crawford dans The Atlantic, les mesures qu'effectuent ces outils dépendent de la façon dont ils ont été programmés et sont souvent imprécises.

« Le Jawbone UP, Nike Fuelband, FitBit and Withings Pulses [différents modèles de bracelets connectés, ndlr] ont chacun des modes de fonctionnement particulier : certains comptabilisent les mouvements de bras comme de la marche (merveilleux, si vous voulez comptabiliser l'écriture comme de l'exercice), d'autres comptabilisent difficilement le vélo comme une activité physique.

La fonction de mesure du sommeil emploie des méthodes assez grossières pour faire la différence entre sommeil léger et sommeil profond. […] »

Un bracelet Jawbone Up (Ashley Baxter/Flickr/CC)

La chercheuse ajoute, faisant référence à l'exploitation de ces données :
« Ces données sont rendues encore plus abstraites par des entreprises d'analytique qui créent des algorithmes propriétaires, pour les comparer à leur standard de ce qu'est une personne normale "en bonne santé." »

Effectivement, explique Me Le Corre, à mesure que l'on s'interroge sur le statut de ces objets, on découvre leurs limites :

« La question de la fiabilité des données de ces objets va se poser de façon aiguë. Pour l'instant, nous manquons de recul sur ces choses-là parce qu'elles sont très récentes. D'où l'intérêt de le soumettre à la discussion des deux parties, qui sert de garde-fou. »

Les données par elles-mêmes ne signifient rien : elles s'intègrent dans un faisceau de preuves, et doivent toujours être contextualisées.

Au-dessus des témoins humains…
En voyant les données de bien-être utilisées contre leur propriétaire, on comprend aussi mieux ce que sont vraiment les objets connectés.
Ainsi, réfléchissant sur ce thème, la chercheuse Kate Crawford, qui travaille sur les implications du big data et des objets connectés, rappelle l'ambiguïté fondamentale des objets connectés :

– ils se présentent comme les instruments d'une meilleure connaissance de soi,
– mais sont aussi des « informateurs », qui collectent des données et les transmettent au fabricant et à des tiers – potentiellement à des assureurs et des employeurs.
[Plus profondément, c'est le statut que l'on veut donner à ces données qui est en jeu. Kate Crawford met en garde contre la tentation d'une « vérité fondée sur les données », où celles-ci finiraient par sembler plus fiables – parce que plus neutres – que l'expérience des témoins.

« Donner la priorité aux données, qui sont irrégulières et peu fiables, sur les témoignages humains, cela signifie que l'on donne le pouvoir à l'algorithme. Or ces systèmes sont imparfaits – comme peut l'être le jugement humain. »

Les données des objets connectées ne sont que ça, des données : des mesures qu'il faut contextualiser et comprendre, et surtout ne pas prendre pour argent comptant.

Source : http://rue89.nouvelobs.com/2015/07/01/quand-les-objets-connectes-temoignent-a-proces-contre-260040

Boulanger, épinglé par la Cnil pour des commentaires sur un fichier client | Le Net Expert Informatique

Boulanger épinglé par la Cnil pour des commentaires sur un fichier client

La Cnil a mis en demeure la société Boulanger, dont les employés ont quelque peu abusé de l'espace libre laissé au sein d'un fichier client. Plusieurs commentaires insultants ont été constatés par la Commission, qui laisse 3 mois à la société pour se mettre en règle.

Peut-on inscrire n'importe quoi dans le champ commentaire d'un fichier client ? Pas vraiment : la Cnil a ainsi annoncé aujourd'hui avoir épinglé l'enseigne Boulanger suite à une plainte lui ayant signalé des commentaires injurieux dans ses fichiers clients.
Sur son site, la Cnil explique avoir effectué un contrôle sur place doublé d'un contrôle en ligne suite à un dépôt de plainte, qui lui a permis de constater des pratiques contrevenant à la loi Informatique et Libertés. « Les fichiers de la société comportaient de nombreux commentaires excessifs sur ses clients, comme par exemple « n'a pas de cerveau », « cliente avec problème cardiaque », « client alcoolique » ou encore des propos insultants » rapporte ainsi la Cnil, qui explique avoir mis en demeure Boulanger, sommé de se mettre en conformité avec la loi sous trois mois.

La Cnil veut faire un exemple
La Cnil explique avoir relevé pas moins de 5828 commentaires désobligeants parmi les fichiers clients de Boulanger. La société est également épinglée pour non-respect des règles encadrant l'usage des cookies : la société manquait à son obligation de prévenir l'utilisateur de l'utilisation de cookies pour le tracking et la Cnil relève également la mise en place « de certains cookies à finalité publicitaire [ayant] une durée de vie pouvant aller jusqu'à 15 ans. »
Pas de chance pour Boulanger, la Cnil explique avoir choisi de mettre en avant cette procédure « afin d'appeler notamment l'attention des entreprises sur la nécessité de ne pas enregistrer de commentaires excessifs dans leurs fichiers clients. » Il fallait faire un exemple et la Cnil précise que cette mise en demeure n'est pas une sanction, mais rappelle que si Boulanger ne se met pas en règle, une nouvelle procédure pourrait être initiée à l'encontre de Boulanger.Via son compte Twitter, la marque s'est excusé et promet de remédier à la situation.

Source : http://www.zdnet.fr/actualites/boulanger-epingle-par-la-cnil-pour-des-commentaires-sur-un-fichier-client-39822914.htm

---

Etude d'impacts sur la vie

privée : découvrez la méthode | Le Net Expert Informatique

17

	Etude d'impacts sur la vie privée : suivez la méthode de la CNIL

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité
La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée
Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :
1.les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;
2.la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Pour mettre en oeuvre ces deux piliers, la démarche comprend 4 étapes :
1.étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
2.étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
3.étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
4.validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

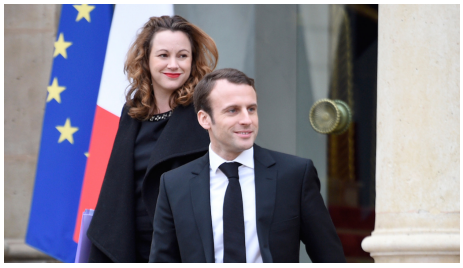
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

PIA, LA MÉTHODE
PIA, L'OUTILLAGE

Source : http://www.newspress.fr/Communique_FR_289793_1332.aspx

---

Bercy devra gérer non pas une, mais deux lois numériques | Le Net Expert Informatique



Bercy devra gérer non pas une, mais deux lois numériques

La loi numérique, tout le monde en parle. Même le chef de l'Etat a abordé le sujet lors de l'interview du 14 juillet. Désormais, il semble probable qu'au lieu d'un texte il y en ait deux. Un signé Macron pour la croissance, l'autre signé Axelle Lemaire pour les libertés.

La question revient à chaque fois qu'un journaliste rencontre un responsable gouvernemental proche du dossier. « Où en sommes-nous de la loi numérique dont on parle depuis 2013 ? » La réponse est toujours la même, ou presque : « Nous y travaillons, nous vous tiendrons informé quand nous aurons avancé ». Rien n'est vraiment officiel mais en fait, il n'y aura pas une loi, mais deux. L'une sur la transformation numérique de l'économie, l'autre sur les libertés individuelles.

Lors de la traditionnelle interview du 14 juillet, le chef de l'Etat y a fait une allusion. « Je vais préparer une loi sur le numérique, tout ce qui est activités nouvelles, tout ce qui peut provoquer de l'emploi ». Le message s'adresse clairement à Emmanuel Macron, ministre de l'économie, de l'Industrie et du Numérique.
Dès le lendemain, lors d'un point presse, le ministre est revenu sur le sujet. Sans entrer dans les détails, il a simplement précisé que les premières propositions seront faites au plus tard début 2016. Et pour calmer les impatients, il a prévenu qu'il prendra le temps nécessaire pour l'élaborer. Et en effet l'exercice promet d'être délicat.
Emmanuel Macron est parfaitement conscient du levier que représente le numérique en matière de création d'emploi. Mais il doit composer entre une nouvelle économie qui bouscule les règles des entreprises traditionnelles. Tandis que ces dernières se trouvent, elles, confrontées à une concurrence qu'elles estiment déloyale, voire illégale selon les cas.

Une loi Macron 2 pour la transformation numérique
Dans son message, François Hollande a été plutôt clair: « il faut qu'il n'y ait rien dans nos règles, dans nos formalités qui puisse entraver ». La guerre entre Uber et les taxis est l'un des exemples les plus frappants de la crainte que génère le potentiel des nouvelles technologies. Ce sera donc à Emmanuel Macron de gérer ce dossier dans une loi qui a déjà un nom: Macron 2.
Autres sujets d'importance, les données personnelles et les libertés individuelles face aux géants du Net. Ces sujets devraient faire parti d'un second texte qui sera cette fois sous la responsabilité d'Axelle Lemaire. Le cœur de ce projet devrait donner plus de poids à la Cnil dont le pouvoir, notamment celui de sanctionner, doit être renforcé. En janvier 2015, sa présidente, Isabelle Falque-Pierrotin faisait déjà des propositions sur le contenu du texte.
Mais la présidente de la Cnil est également présidente des Cnil européennes, connues sous le nom de « Groupe de l'article 29 » et dans ce cadre, elle rappelle que le texte devra être compatible avec le projet de règlement européen. « La législation sur les données personnelles ayant une portée économique croissante, les modifications éventuelles ne doivent pas créer de distorsion entre pays de l'Union. » Le cadre est posé. Reste désormais à savoir quand Axelle Lemaire présentera cette loi. Avant ou après celle d'Emmanuel Macron?

Source : http://bfmbusiness.bfmtv.com/entreprise/bercy-devra-gerer-non-pas-une-mais-deux-lois-numeriques-902051.html
Par Pascal Samama

Android : Google Photos charge les clichés même après une désinstallation | Le Net Expert Informatique

Android : Google Photos charge les clichés même après une désinstallation

Google continue de charger sur ses serveurs les clichés capturés avec un smartphone Android même lorsque l'application Google Photos a été désinstallée.

A l'occasion de la conférence I/O, Google lançait un nouveau service baptisé Google Photos. Ce dernier, désormais dissocié de Google+, propose un espace de stockage illimité et se présente sous la forme d'une application mobile pour Android et iOS. Google est ainsi paré pour entrer en concurrence avec Facebook, Flickr, Microsoft ou Apple sur le domaine de la photo sur mobiles.
Sur le système d'exploitation Android, les développeurs ont choisi de ne pas placer les options de ce nouveau service directement au sein de l'application Google Photos mais de les ajouter dans les paramètres du compte Google. Cela signifie qu'un internaute désinstallant l'application après l'avoir testé devra effectuer une manipulation supplémentaire pour stopper le service. En effet, le magazine Nashville Business Journal explique qu'une fois l'application installée et activée, elle ajoute une option permettant d'autoriser le chargement des clichés vers les serveurs de Google. Mais lorsque Google Photos est désinstallée, l'option est toujours présente et bel et bien activée. Reste à savoir si dans une prochaine mise à jour Google rectifiera le tir.
Rappelons qu'avec Google photos, les clichés ne peuvent être publiés en privé. Google les masque en leur attribuant des URL supposées « indevinables », qu'il est possible de partager vers un tiers. Le dispositif a été révélé lorsqu'un internaute a réussi à accéder à ses photos supposées privées sans se connecter à son compte Google. Selon la firme de Mountain View, ces URL d'une quarantaine de caractères, seraient plus complexes qu'un mot de passe traditionnel.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.clubic.com/application-mobile/actualite-773600-android-google-photos-chargement-photos-desinstalaltion.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1067015562#pid=22889469

Prévention des risques : les

dispositifs d’alerte à la population | Le Net Expert Informatique

Face aux risques (inondation, canicule, attaque terroriste, incident nucléaire, épidémie…) susceptibles de mettre en danger les populations, les maires peuvent constituer deux registres nominatifs destinés à faciliter les secours. La Commission nationale de l'informatique et des libertés (Cnil) fournit un cadre à la constitution de ces registres qui ne doivent pas être prétextes à la création de « fichiers de population ».

L'utilisation des ces registres est strictement limitée aux secours déclenchés par le maire en cas d'alerte. Les habitants doivent avoir sollicité leur inscription par une démarche volontaire.

Pour la collecte des informations nécessaires, la Cnil a établi deux formulaires :
l'un au titre du « plan d'alerte et d'urgence au profit des personnes âgées et des personnes handicapées en cas de risques exceptionnels ». Il s'agit d'une reprise du « registre canicule » prévu par le décret n° 2004-926 « canicule », abrogé par le décret n° 2005-1135 ; (http://www.courrierdesmaires.fr/wp-content/uploads/2015/06/plan-urgence-formulaire-collecte-modele.doc)
l'autre au titre du « plan communal de sauvegarde » (PCS), dispositif d'alerte générale à la population pour faire face à la réalisation de risques connus auxquels est soumis un territoire communal (décret n°2005-1156).
(http://www.courrierdesmaires.fr/wp-content/uploads/2015/06/pcs-formulaire-collecte-modele.doc)
Les registres de population ainsi constitués collectent donc des données personnelles volontairement transmises par les personnes concernées. Celles qui n'y sont pas inscrites ne sont évidemment pas exclues du bénéfice des secours qui seront alors déclenchés.
A noter. Si la collecte de données de santé, souvent constatée, est par principe excessive et passible de sanctions pénales, une description objective des capacités des personnes sur ces registres semble néanmoins pertinente afin de prévoir le mode d'évacuation et le matériel de premiers secours.

Le maire, responsable de traitement, doit garantir la confidentialité et la sécurité des données. Toute personne accédant aux données du registre est tenue au secret. Les données personnelles ne peuvent en aucun cas être utilisées à d'autres fins que celle de constituer et déclencher le dispositif d'alerte.

Source :
http://www.courrierdesmaires.fr/51257/prevention-des-risques-les-dispositifs-dalerte-a-la-population/

Avis trimestriel N° 02-2015 de la Commission de protection des données personnelles du Sénégal (CDP) | Le Net Expert Informatique

Avis trimestriel N° 02-2015 de la Commission de protection des données personnelles du Sénégal (CDP)

Le présent avis trimestriel de la CDP concerne la période allant du 1er avril au 30 juin 2015. Il décrit les activités au sein de la Commission et les constats sur le traitement des données personnelles par les acteurs des secteurs public et privé au Sénégal.

La Commission publie ainsi ledit avis trimestriel conformément à l'article 43 de son Règlement intérieur et après en avoir délibéré en sa séance plénière du 10 juillet 2015.

1 – Compte rendu des activités :
Au cours de ce deuxième trimestre 2015, la CDP a constaté une meilleure prise de conscience des responsables de traitement. En effet, 38 structures se sont rapprochées de l'Autorité de protection afin de mieux s'imprégner de la législation et de connaitre leurs obligations déclaratives.
La Commission a traité 134 dossiers dont 89 déclarations et 45 demandes d'autorisation. A l'issue des 06 sessions plénières, les commissaires ont délivré 54 récépissés de déclaration et 28 autorisations.
Au titre des signalements et des plaintes, la CDP a enregistré l'usage illégitime de numéros courts, une arnaque sur le réseau d'un opérateur de télécommunications, la collecte non autorisée d'empreintes digitales dans un système financier décentralisé, la diffusion de fausses nouvelles, l'arnaque et le chantage sur le net, l'utilisation abusive et sans autorisation de photos et la publication dans la presse de données personnelles d'employés sans leur consentement. Ces cas d'atteinte à la vie privée ont donné lieu à des demandes d'explication qui ont abouti à des déclarations et régularisations devant la CDP. Par ailleurs, la CDP a prononcé un (01) avertissement à l'endroit d'une structure pour envoi répété de courriels et de SMS non sollicités sans mise à disposition d'une possibilité de désabonnement fonctionnel.
Dans le cadre de sa mission de sensibilisation, la Commission a initié des visites de courtoisie auprès d'acteurs institutionnels. C'est ainsi qu'elle a été reçue par la Cellule Nationale de Traitement des Informations Financières(CENTIF), l'Agence nationale de la Banque Centrale des Etats de l'Afrique de l'Ouest(BCEAO), l'Office national de Lutte contre la Fraude et la Corruption(OFNAC) et en fin le Conseil Economique Social et Environnemental(CESE). De même, la phase pilote de la campagne de sensibilisation ''Internet, c'est moi qui décide'' a été lancée en partenariat avec la société Computech Groupe au sein d'établissements secondaires de Dakar.
Enfin, la CDP a organisé un Forum africain sur la protection des données personnelles (FAPDP 2015) à Dakar les 19 et 20 mai 2015. Cet évènement a enregistré la participation de plus de 350 personnes dont des autorités de protection de 13 pays africains (33 délégués), le Conseil de l'Europe et l'Association francophone des autorités de protection des données personnelles (AFAPDP).

2 – Observations /constats :
A l'examen des dossiers reçus à la CDP, des manquements ont été relevés dans le traitement des données personnelles de quelques structures.

Du point de vue juridique, on note :
• l'installation dans un lieu de travail d'un nombre disproportionné de caméras de surveillance;
• le non-respect des conditions de la prospection directe notamment, les droits des personnes concernées (consentement, opposition, etc.) ;
• le non accomplissement des formalités déclaratives devant la CDP préalables au traitement des données ;
• la durée illimitée de conservation des données traitées ;
• l'absence d'engagement de confidentialité entre le responsable de traitement et son sous-traitant.

Sur le plan technique, la pratique de l'externalisation reste une préoccupation pour la Commission. Cette situation constitue un défi supplémentaire pour la protection des données en ce sens que le responsable de traitement n'a plus le total contrôle de son système d'information.

Concernant le traitement des données sensibles comme les données de santé et la biométrie, les responsables de traitement devraient mettre une authentification forte au lieu de recourir simplement à un login et un mot de passe.

Enfin, il a été relevé dans certaines structures, l'absence de politique formalisée d'accès aux données et de mécanismes de sensibilisation des usagers sur les mesures de sécurité mises en place. Il est important que de telles dispositions soient prises par le responsable de traitement conformément à l'article 71 de la loi n° 2008-12 du 25 janvier 2008 portant sur les données à caractère personnel et la délibération n°2014-014/CDP du 3 avril 2014 portant sur les mesures de sécurité applicables aux traitements des données à caractère personnel.

3 – Recommandations :
Au regard des constats à l'examen des dossiers instruits, la CDP formule au profit de toutes les parties prenantes, les responsables de traitement du secteur public, du secteur privé, des organismes de la société civile et autres acteurs, les recommandations suivantes :

• Préciser le lieu exact (ville ou pays) de stockage du serveur contenant les données selon qu'il appartient à la structure ou à l'hébergeur (serveur mutualisé, serveur dédié);
• Signer obligatoirement un engagement de confidentialité en cas d'intervention d'un tiers dans le système mis en place afin d'augmenter le niveau de sécurité des données;
• Utiliser un langage codé et accessible uniquement au corps médical pour les dossiers de santé et mettre en place une authentification forte dans le cadre de la collecte de données de santé;
• Informer les personnes concernées de la présence de caméras de vidéosurveillance (affiches avec indication du numéro du récépissé de la CDP, panneau de signalement) et veiller à positionner les caméras uniquement sur les parties communes et s'assurer que les parties privées ne soient pas filmées;
• Désinscrire gratuitement et systématiquement, dans le cadre de la prospection commerciale, les personnes qui en font la demande avec effet immédiat;
• Veiller à assurer une protection des données transférées dans des serveurs à l'étranger en mettant en place des mécanismes de sauvegarde et de réplication/duplication;
• Recueillir le consentement, libre et éclairé des personnes qui font l'objet de prospection, tout comme le consentement des personnes concernées avant toute publication ou communication à des tiers de leurs données personnelles (photos, vidéos, etc.);
• Ne pas publier dans la presse des décisions individuelles mettant en cause les employés/salariés sans leur consentement;
• Saisir la CDP pour la suppression de tout contenu pouvant nuire à la réputation des personnes;
• Etre prudent sur les informations à communiquer sur les réseaux sociaux;
• Se rapprocher de la CDP pour une meilleure connaissance de la législation sénégalaise sur la protection des données personnelles.

Source : http://www.actusen.com/avis-trimestriel-n-02-2015-de-la-commission-de-protection-des-donnees-personnelles-du-senegal-cdp/#

Hyperconnexion du corps humain : 3 règles pour ne pas faire n'importe quoi | Le Net Expert Informatique

Hyperconnexion du corps humain : 3 règles pour ne pas faire n'importe quoi

Face au déploiement des objets connectés au corps humain, qui permettent de recueillir des données de santé, utilisateurs et industriels doivent être particulièrement vigilants, nous explique Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI.

Bracelets, montres, balances connectés… la m-santé envahit les magasins spécialisés. Au-delà de leur côté ludique, ces objets permettent aux entreprises de recueillir de très nombreuses données sur leurs utilisateurs : rythme cardiaque, nombre de pas effectués par jour, quantité et qualité du sommeil, taux de sucre dans les larmes, taux d'alcoolémie ou tension artérielle…
Ce mouvement de collecte massive de données – le big data – n'en est qu'à son début, selon la Cnil. En 2017, un utilisateur de smartphone sur deux aura installé au moins une application dédiée à son bien-être et à sa santé.

Les données recueillies sont traitées par de nombreuses entreprises qui les exploitent afin de mieux connaître leurs clients. Une pratique intrusive, qui doit susciter la vigilance des utilisateurs, mais aussi des industriels. En effet, leur responsabilité peut-être engagée. Les données recueillies, liées à la santé, ont un caractère sensible et font l'objet d'une protection renforcée. Ainsi, leur collecte et leur traitement, soumis à un contrôle accru, doivent être autorisés. Mais certaines data -celles se rapportant en général au bien-être-, échappent à une demande d'autorisation préalable grâce aux normes simplifiées. Attention cependant car la frontière entre bien-être et santé est particulièrement ténue.

Pour assurer leur sécurité juridique, les industriels du secteur mettre en place quelques règles.
1. RESPECTER LE CADRE LÉGAL ET LE RAPPORT DE LA CNIL SUR LA PRATIQUE DU « QUANTIFIED SELF »
Le rapport de la Cnil, déposé fin mai 2014, intitulé 'Le corps, nouvel objet connecté', traite des problèmes liés aux données personnelles de santé issues des applications et objets de mesure de soi (quantified self). Ces pratiques consistent généralement à mesurer et à comparer avec d'autres, des variables de notre mode de vie (nutrition, exercice physique, sommeil…). La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques.

Le « quantified self » constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La Cnil s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente – et face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles – les industriels développant des produits liés à la santé doivent veiller à rester dans les clous lors de la collecte.

2. MISER SUR LE « CLIENT EMPOWERMENT » POUR GAGNER LA CONFIANCE DES CONSOMMATEURS
Ce mouvement donne davantage de pouvoirs de contrôle au client. Il permet de rééquilibrer la relation entre l'entreprise collectrice de données et l'usager qui a souvent l'impression d'être négligé par les professionnels. Cette prise de pouvoir peut aussi permettre la patrimonialisation des données à condition d'obtenir le consentement direct du client. Cela ouvre aux industriels la possibilité de commercialiser les données collectées.

3. SE CONFORMER AUX PRINCIPES DE « PRIVACY BY DESIGN »
Le concept de « privacy by design » propose de faire de la protection de la vie privée de l'utilisateur une caractéristique majeure de l'objet afin « d'assurer la protection de la vie privée en l'intégrant dans les normes de conception des technologies, pratiques internes et infrastructures matérielles ». Les données recueillies ne sont alors pas extensivement partagées ou revendues. En intégrant ce concept au cahier des charges de l'objet connecté, l'industriel gagnera la confiance des clients et se démarquera aussi de ses concurrents.

TOUT N'EST PAS PERMIS
La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques. Elle constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont ainsi déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La CNIL s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente, face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles, les industriels développant des produits liés à la santé doivent tenir compte du fait que tout n'est pas permis.

Source : http://www.usine-digitale.fr/article/hyperconnexion-du-corps-humain-3-regles-pour-ne-pas-faire-n-importe-quoi.N335953
Par Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI

Cookies et tracking : la Cnil a mis en demeure une vingtaine de sites | Le Net Expert Informatique

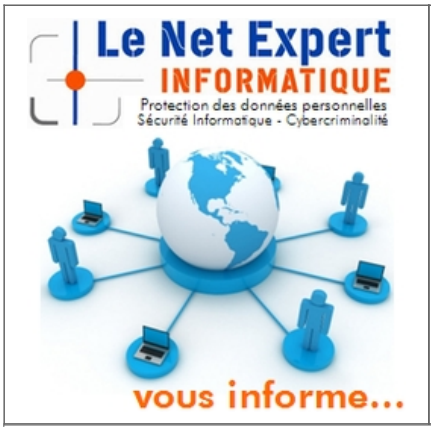
La Cnil publie un premier bilan de ses contrôles sur l'application de la loi relative aux cookies et au tracking publicitaire sur les sites web. La Commission a mis en demeure une vingtaine de sites qui se contentent d'informer l'utilisateur mais ne prennent pas en compte son consentement.

Manifestation la plus visible des évolutions autour des données personnelles : aujourd'hui, les sites qui vous traquent et ont recours à des cookies prennent la peine de vous le dire. Depuis un peu plus d'un an, l'entrée en vigueur des lois européennes a poussé de nombreux sites web à signaler aux utilisateurs qu'ils avaient recours à des cookies et autres outils de traçage des utilisateurs dans un but commercial, le plus souvent grâce à un bandeau s'affichant sur le site lors de la première visite.
Mais pour la Cnil, cela ne suffit pas. En effet la commission Nationale Informatique et Liberté explique dans son bilan avoir mis en demeure une vingtaine d'éditeurs de se mettre en conformité avec la loi dans un délai déterminé. En effet, la Cnil rappelle qu'il ne s'agit pas uniquement d'informer l'utilisateur mais bien de recueillir le consentement avant de déposer les cookies, et donc d'offrir à l'internaute la possibilité d'opt-out lors de sa visite du site.

Bientôt plus de contrôles
« En effet, si certains sites ont apposé un bandeau informant les internautes que des cookies sont déposés sur leur ordinateur, aucun des sites contrôlés n'attend d'avoir recueilli le consentement des internautes avant de déposer lesdits cookies. » La Cnil précise également que renvoyer l'internaute aux paramétrages de son navigateur n'est pas une attitude valable à l'égard de la loi.
Au cours de l'année 2014, la Cnil a effectué au total 24 contrôles sur place, 27 contrôles en ligne et deux auditions afin de s'assurer du respect des règles en vigueur. Et la Commission entend bien poursuivre sur sa lancée : elle a récemment annoncé vouloir augmenter le nombre de ses contrôles sur les domaines relevant de sa juridiction. La Cnil tiendra notamment une session de question/réponse sur ce sujet aujourd'hui à 13h via son compte Twitter, @Cnil.

Source : http://www.zdnet.fr/actualites/cookies-et-tracking-la-cnil-a-mis-en-demeure-une-vingtaine-de-sites-39821796.htm

La Cnil interdit la géolocalisation du salarié en dehors du temps de travail | Le Net Expert Informatique



La Cnil interdit la géolocalisation du salarié en dehors du temps de travail

Par une délibération du 4 juin 2015, la Cnil a décidé de renforcer l'encadrement du recours au dispositif de géolocalisation.

La Commission nationale de l'informatique et des libertés (Cnil) constate le développement de dispositifs dits de géolocalisation permettant aux organismes privés ou publics de prendre connaissance de la position géographique, à un instant donné ou en continu, des employés par la localisation des véhicules mis à leur disposition pour l'accomplissement de leur mission. Ainsi, l'employeur peut contrôler le respect des règles d'utilisation d'un véhicule par ses employés grâce à la géolocalisation.
Ce dispositif permet de collecter des données à caractère personnel et sont donc soumis aux dispositions de la loi du 6 janvier 1978.
Par délibération n° 2015-165 du 4 juin 2015, la Cnil a considéré qu'il était nécessaire de compléter la norme permettant de simplifier la déclaration des traitements visant à géolocaliser un véhicule utilisé par un employé.
Dans cette délibération, la Cnil précise que le recours au dispositif peut servir à justifier la réalisation d'une prestation auprès d'un client ou d'un donneur d'ordre, ou bien à lutter contre le vol du véhicule.
En outre, la Cnil interdit formellement aux employeurs de collecter des données de localisation en dehors du temps de travail du salarié, à savoir lors de ses temps de pause et du trajet entre son domicile et le lieu de travail.
La faculté de désactiver la fonction de géolocalisation doit être laissée à l'employé. Toutefois, la Cnil souligne que des explications pourront être demandées au salarié lorsque les désactivations sont trop longues ou trop fréquentes.
Enfin, les employeurs publics et privés devront se conformer au nouveau dispositif avant le 17 juin 2016.

Source : http://droit-public.lemondedudroit.fr/droit-a-entreprises/droit-social/206288-la-cnil-interdit-la-geolocalisation-du-salarie-en-dehors-du-temps-de-travail.html